THE NATIONAL CYBERSECURITY SOCIETY

BUSINESS IDENTITY THEFT IN THE U.S. FACT SHEET

VICTIM RESOURCES

Do you think your business has been the victim of identity theft? Not sure where to start or what to do? This fact sheet provides some guidance and a list of resources. It is important to note that the procedures for addressing business identity theft are different than consumer identity theft. The FTC only responds to consumer complaints and the credit reporting agencies won't place a "freeze" on your account like they would for consumers. So, the traditional advice on how to respond to identity theft doesn't apply to businesses.

As with any cyber incident, the first task is to figure out what happened. Interview staff, investigate and **take notes** – the goal is to document what occurred, how you found out, and collect evidence. Identify what accounts were affected, who has access to those accounts, when was the last time the account was accessed and/or when a transaction occurred. Check if other accounts have been affected. These are all examples of good data to collect. **Change passwords to these accounts immediately.**

Financial Fraud. If your credit card or line of credit was stolen, the next step is to notify the financial institution and put a freeze on the account. Once this has been done, you may need to obtain funds from another creditor in order to provide the operating funds until the account freeze is lifted. The analysis you conducted initially will be helpful when you contact the financial institution. As a business owner, many banks will require you to prove you or your employees were not the cause of the fraudulent charge. Your financial institution will guide you through the process, albeit a long one.

Credit Reporting Agencies. Next step is to contact Dun and Bradstreet's fraud department at 1-866-895-7262, highriskandfraudinsight@dnb.com and report the theft. D&B will investigate the issue, confirm the information in question and correct any inaccuracies in your account. In many cases a "stop distribution" order will be placed on the account until the matter is resolved. The stop distribution or account freeze is shared with the other CRAs (Experian and Equifax, not TransUnion) who will flag your business credit file. This may affect your ability to obtain any additional credit. (TransUnion only manages credit files for consumers, not businesses.)

Tax Fraud. If you have been notified by the IRS that your business has been involved in a fraudulent tax return activity, they will guide you on the information they may need to conduct the investigation. They will only notify you **by mail**, not phone. Don't fall victim to IRS phone scams! If, however, you notice that someone has used your business to submit a fraudulent tax return, notify the IRS at 1-800-829-4933.

Law Enforcement. Local law enforcement is required to respond to the incident. Call the non-emergency number to report the crime – reporting the crime will be helpful for insurance purposes. Ensure you obtain a copy of the incident report. Unfortunately, the crime may never be solved.

Internet Crime Complaint Center (IC3). Businesses can file a complaint at https://www.ic3.gov/default.aspx. IC3 doesn't investigate crimes, but collects valuable statistics on Internet crime. Of particular, IC3 is interested in crimes related to website/online extortion, identity theft, intellectual property rights, hacking, and theft of trade secrets.

State Business Registries. Many states offer resources for business identity theft. Visit your state's website for information or resources for victims.

Identity Theft Resource Center (ITRC). The ITRC offers many free resources for victims of identity theft. While the business might have been the target of this crime, owners and employees often feel victimized as well. Visit their site at: https://www.idtheftcenter.org/